ABSTRACT OF THE DISCLOSURE

A method and apparatus for securely communicating ephemeral information from a first node to a second node. In a first embodiment, the first node encodes and transmits an ephemeral message encrypted at least in part with an ephemeral key, from the first node to the second node. Only the second node has available to it the information that is needed to achieve decryption by an ephemeral key server of a decryption key that is needed to decrypt certain encrypted payload information contained within the message communicated from the first node to the second node. In a second embodiment the first node transmits to the second node an ephemeral message that is encrypted at least in part with an ephemeral key. The ephemeral message includes enough information to permit the second node to communicate at least a portion of the message to an ephemeral key server and for the ephemeral key server to verify that the second node is an authorized decryption agent for the message. After verifying that the second node is an authorized decryption agent for the message, the ephemeral key server returns to the second node an encrypted decryption key that is needed to decrypt the encrypted message. The ephemeral message may comprise an encrypted decryption key that may be used after decryption of the decryption key to decrypt other encrypted information communicated to the second node.

241821

ATTORNEY DOCKET NO. P5761
WEINGARTEN, SCHURGIN,
GAGNEBIN & HAYES, LLP
TEL. (617) 542-2290
FAX. (617) 451-0313